

Relatório ESA e seguimento da expansão da retenção de dados

Índice

[Introdução](#)

[Pré-requisitos](#)

[Relatando dados](#)

[Seguindo dados](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como aumentar o relatório e retenção de dados do seguimento na ferramenta de segurança do email de Cisco (ESA) a fim permitir a sobreposição dos dados.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- Dispositivo do Gerenciamento de segurança do índice de Cisco (S A)

Relatando dados

Quando um S A é autônomo ou inacessível, o ESA começa a enfileirar dados do relatório. O ESA retém à revelia 100 arquivos, cada um com uma duração 15-minute. Essencialmente, o ESA retém dados para a corrente 1,500 minutos (15 x 100), que é equivalente a 25 horas. Se o S A está para baixo por 30 horas, a seguir você perde os dados do relatório para as primeiras horas 5 (30 horas - 25 horas).

Use a informação neste exemplo a fim aumentar o número de arquivos que são retidos no ESA:

```
example.com> reportingconfig
```

```
Choose the operation you want to perform:
```

- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.

```
[> mailsetup
```

```
SenderBase timeout used by the web interface: 2 seconds
```

```
Sender Reputation Multiplier: 3
```

```
The current level of reporting data recording is: unlimited
```

```
No custom second level domains are defined.
```

```
Legacy mailflow report: Disabled
```

```
Choose the operation you want to perform:
```

- SENDERBASE - Configure SenderBase timeout for the web interface.
- MULTIPLIER - Configure Sender Reputation Multiplier.

- COUNTERS - Limit counters recorded by the reporting system.
- THROTTLING - Limit unique hosts tracked for rejected connection reporting.
- TLD - Add customer specific domains for reporting rollup.
- STORAGE - How long centralized reporting data will be stored on the C-series before being overwritten.
- LEGACY - Configure legacy mailflow report.

[> **storage**

While in centralized mode the C-series will store reporting data for the M-series to collect. If the M-series does not collect that data then eventually the C-series will begin to overwrite the oldest data with new data.

A maximum of 24 hours of reporting data will be stored.

How many hours of reporting data should be stored before data loss?

[24]> **30**

Seguindo dados

Similarmente, quando o S A é autônomo ou inacessível, o ESA começa a enfileirar o seguimento de dados. O ESA retém 60 arquivos, cada um com uma duração de três-minuto.

Conseqüentemente, o ESA retém os dados para os 180 minutos passados (60 x 3). Todos os dados de seguimento que não forem recuperados do ESA e são mais velhos de três horas são perdidos.

Use a informação neste exemplo a fim aumentar o número máximo de seguir arquivos:

example.com> **trackingconfig**

Choose the operation you want to perform:

- MODE - Set whether tracking is run on box or centralized.

[> **storage**

While in centralized mode the C-series will store tracking data for the M-series to collect. If the M-series does not collect that data then eventually the C-series will begin to overwrite the oldest data with new data.

A maximum of 60 files are presently stored. This means a maximum of 3 hours will be stored, though depending on load that time may be smaller.

How many files should be stored before data loss?

[60]> **500**

Informações Relacionadas

- [AsyncOS para Guias do Usuário da Segurança do email](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)